UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/689,549	10/21/2003	Joona Airamo	060258-0306460	9315

909 7590 10/04/2007

PILLSBURY WINTHROP SHAW PITTMAN, LLP
Eric S. Cherry - Docketing Supervisor
P.O. BOX 10500
MCLEAN, VA 22102

EXAMINER	
HOMAYOUNMEHR, FARID	
ART UNIT	**PAPER NUMBER**
2132	

MAIL DATE	DELIVERY MODE
10/04/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/689,549	AIRAMO, JOONA	
	Examiner	Art Unit	
	Farid Homayounmehr	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 July 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communications: application, filed 10/21/2003; amendment filed 7/12/2007.

2. Claims 1-15 are pending in the case.

Response to Arguments

3. Applicant argues: "However, Jain fails to teach or suggest checking whether a relationship between a port and a device and a control connection fulfills predefined criteria." However, as shown in the First Office Action, per parag 31 to 38, the main (control) channel and the additional FTP channels and ports are identified by the firewall, and a policy is enforced. The policy is the predefined criteria.

Applicant further argues: "Further, Jain fails to teach or suggest conditionally blocking such a related connection, if the port of the device does not fulfill the pre-defined criteria." However, as shown in Jain paragraphs 138 and 139, one of the enforced policies is blocking the connection.

Applicant further argues: "Thus, Jain fails to teach or suggest the claimed invention whereby, malicious related connections are detected and blocked by examining relationships between a

port negotiated for a related connection and the associated control connection, and by deciding on the basis of this relationship, whether the related connections shall be allowed." However, first, there is no requirement in the claims to detect malicious related connections. Second, as discussed above, Jain teaches blocking in connection based on the relationship between the ports and control connection, and blocking the connection based on a policy.

Applicant further argues: "Accordingly, Jain fails to teach or suggest the claimed invention embodiments wherein a port of a device is opened within a predefined time window in relation to noticing negotiation of a related connection within the control connection. Similarly, Jain fails to teach or suggest the claimed invention embodiments wherein a control connection and the port of a device are both opened using the stone process family." However, the rejections presented in the first office action show how the cited claim requirements are taught by Jain, or the combination of Jain and Hall, and applicant does not provide any reason to traverse the rejections.

Applicant further argues: "The Office Action asserted that Jain's Fig. 1 illustrates a classification tree. However, the classification tree in Jain's Fig. 1 does not depict processes; rather it depicts protocols." However, the classifier determines the parent processes of connections (as defined by specification, when two processes have the same parent process, they are in the same process family). As shown in Fig. 1, the FTP process

itself and the Dynamic TCP port from FTP have a parent process, identified by Jain's classifier (the TCP process).

With regards to claim 2 and the Hall reference, applicant argues: "As illustrated in Fig. 2, for example, there is a connection between the client and the target server. Thus the monitoring server does not monitor the traffic between the client and the target server or control whether a connection to the target server is allowed." However, a connection shown in Fig. 2 does not mean that Hall does not perform any monitoring on the connection. As a matter of fact, Hall teaches a system for detecting intrusion (abstract), which enforces a policy of requiring a response to a command to be received in a predetermined time interval. Parag. 24 to 27 describe initiation of an FTP connection, which is monitored and allowed to complete if the response to an initiation is received within a time interval (see Fig. 2, time interval between T1 and T2). Therefore, Hall teaches monitoring a connection. Therefore, Hall teaches enforcing a security policy associated with a FTP connection in requiring a response to a command to be received in a predetermined time interval. Therefore, combination of Hall and Jain makes all claim requirements obvious.

Applicant further argues: "Moreover, one of ordinary skill in the art could not have combined the teachings of Jain and Hall to provide the claimed invention. Hall's time interval TI-T2 referred to by the Office Action, is not in any way related to a setup of a connection; rather, that time interval determines an administrative period of time for which the client is authorized to use

the latent software in the target server. This time may be days, months, or even longer." However, Hall teaches a system for detecting intrusion (abstract), which enforces a policy of requiring a response to a command to be received in a predetermined time interval. Jain teaches the process of checking a connection, and blocking it if the connection is not in compliance with a policy. Therefore, the combination of Hall and Jain teaches all claim requirements.

Applicant further argues: "Moreover, the teachings of Hall are not applicable to Jain's firewall, which in situated between a client and a target server to handle processing PDUs. This is because Jain does not relate to software executed on a target server. Accordingly, if one of ordinary skill in the art had applied the teachings of Hall to Jain's system, the result would have merely provided a further monitoring server and a target server configured to ask permission to execute certain software." However, Hall's system monitors software processes executed on the target server. As shown in the rejections, one example of the software (process) executed on the target server is the FTP process, which creates connections between the target server and the clients. Therefore, combining Hall's Monitoring Server, which monitors an FTP connection with Jain's Firewall, which also monitors connections such as FTP would be obvious to the one skilled in art. Note also that Hall's system is also situated between the clients and the target (see Fig. 5, where the Monitoring Server 26 is connected to the clients 32 and 34 and the target server 22).

Based on the discussion above, applicant's argument relative to the allowability of the pending claims is found non persuasive. The ground of rejection has not been changed and is as follows:

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1, 6, 8, 13, 14 are rejected under 35 U.S.C. 102(e) as being anticipated by Jain et al. (US Patent Application Publication No. 2003/0131116, filed June 21, 2002).

5.1. As per claim 1, Jain is directed to a method of securing a device having data communication capability (Fig. 2 and associated text shows a firewall, which secures the network device that sends packets received at item 202), comprising dynamically detecting a control connection, which originates from said device (parag. 18-20, where the dynamically negotiated ports are identified by the stateful firewall. Note that parag.

4-6 examples an FTP connection, which dynamically allocates ports and uses them. FTP connections inherently initiate a control channel and a data channel (see Charavarty parag. 37-40 as evidence)), noticing negotiation of a related connection within said control connection, said negotiation comprising at least defining a port of the device for said related connection (parag 31 to 38, where the main (control) channel and the additional FTP channels and ports are identified by the firewall), checking if relationship between said port of the device and the control connection fulfills predefined criteria, and conditionally blocking said related connection, if said port of the device does not fulfill said predefined criteria (parag. 45 shows that the dynamically negotiated FTP channel is fully identified (ports associated with the control channel identified as described above), and a policy is enforced. The policy is the predefined criteria, and as described in parag. 138-139, enforcing includes conditionally blocking the connection).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 2-5, 7, 9-12, 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jain and further in view of Hall (US Patent Application Publication No. 2004/0054928, filed June 17, 2002).

7.2. As per claim 2, Jain is directed a method according to claim 1. However, Jain does not explicitly discuss the criteria, wherein the predefined criteria requires that said port of the device is opened within a predefined time window in relation to noticing negotiation of a related connection within said control connection.

Security policies commonly require a response to an initiation command to be received within a predefined time interval. This is to mitigate attacks such as masquerading or spoofing, where a response from the authorized server is stolen and replaced by attacker's response. As an example, Hall teaches a system for detecting intrusion (abstract), which enforces a policy of requiring a response to a command to be received in a predetermined time interval. Parag. 24 to 27 describe initiation of an FTP connection, which is monitored and allowed to complete if the response to an initiation is received within a time interval (see Fig. 2, time interval between T1 and T2).

Jain teaches a stateful firewall that monitors and identifies an FTP connection and the negotiated ports, and allows configuration of a policy to enforce security of the FTP connection based on the identified elements of the connection. Hall shows that an FTP connection is monitored to verify if the response to a connection initiation is received

within a predetermined time interval. Therefore, it would have been obvious to a person skilled in art to combine Jain and Hall, and set a policy (criteria) in Jain's system to only allow the connection to proceed if the response to an initiation command (opening of the port) is received within a time interval from when the initiation command (control channel) was sent.

The motivation to do so is prevention of spoofing attacks, which relies on blocking the response from the authorized device and replacing it with a response form the attacker.

7.3. As per claim 3, Jain is directed method according to claim 1, wherein said predefined criteria requires that said control connection and said port of the device are opened by the same process family (Jain teaches a tree based classifier, which determines the parent processes of connections (as defined by specification, when two processes have the same parent process, they are in the same process family). As shown in Fig. 1, the FTP process itself and the Dynamic TCP port from FTP have a parent process, identified by Jain's classifier (the TCP process). As shown in parag. 39 and 45, Jain enforces a common policy based on classification tree, and a common policy is to allow a connection initiated by the same process (TCP)).

7.4 As per claim 4, Jain is directed method according to claim 1, wherein said device is running an applet (running applets are inherent in web applications, which is taught as part of Hall's system).

7.5. As per claim 5, Jain is directed method according to claim 4, wherein said control connection originates from the applet See response to claim 4, and note that web clients inherently originate an FTP connection using applets).

8. Limitations of claims 6-15 are substantially the same as limitations of claims 1-5 above.

Conclusion

9. **THIS ACTION IS MADE FINAL,** as no new ground of rejection is included. See MPEP § 7.39. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is (571) 272-3739. The examiner can be normally reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Farid Homayounmehr

9/28/2007

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100